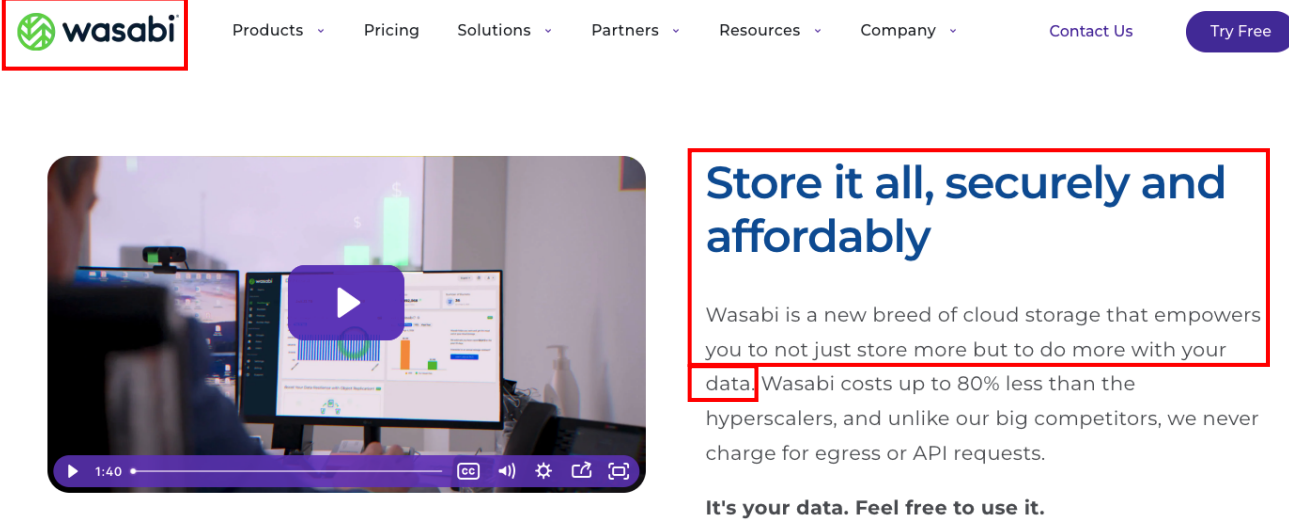# EXHIBIT B

U.S. Patent No. US 8,856,221 v. Wasabi Technologies LLC

1. Claim Chart

Claim	Analysis
[7.P] A method for storing media content and delivering requested media content to a consumer device, the method comprising:	Wasabi Technologies LLC ("Company") performs and/or induces others to perform a method for storing media content and delivering requested media content to a consumer device. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, Company provides a cloud storage solution that enables users to store various types of data, including text, photos, and videos ("media content"), on the Wasabi Cloud. Additionally, Wasabi integrates NirvaShare, a third-party file-sharing and access management solution that allows users to securely manage, share, view ("delivering requested media content"), and download ("storing media content") files directly from the Wasabi Cloud via a dedicated user interface on their device ("consumer device"). Source: https://wasabi.com/cloud-object-storage

WASABI HOT CLOUD STORAGE (Console)

Updated on 06 Nov 2024 · 3 Minutes to read   Print   Share   PDF

Wasabi Hot Cloud Storage is a cloud-based object storage service for a broad range of applications and use cases.

Wasabi Hot Cloud Storage provides a simple web service interface that is 100% Amazon S3 bit-compatible. Wasabi can store and retrieve any amount of data at any time from anywhere on the web. Because Wasabi is highly scalable and you only pay for what you use, developers can start small and grow their applications as they wish, with no compromise to performance or reliability.

Wasabi allows you to store virtually any kind of data in any format. For more detail, review Wasabi's Terms of Use Agreement.

Wasabi Hot Cloud Storage is designed for individuals and organizations that require a high-performance, reliable, and secure data storage infrastructure at minimal cost. The following guides will help you get started and delve deeper into Wasabi features. Refer to the information below these lists for general insight into Wasabi Hot Cloud Storage.

Source: https://docs.wasabi.com/v1/docs/wasabi-cloud-storage-console-1

3

◁ nirvashare   Get Started   White Papers

Secure File Sharing & Access Management Solution For Your Object Storage

A self hosted server for secure file Sharing and Collaboration from Object Storages such as AWS S3, Azure Blob, GCP, DigitalOcean Spaces, MinIO and many more in a most simplified way.

Supports a variety of authentication options while sharing files with users such as SSO with Multi-Factor, Basic, Form and OTP based with granular access control.

Source: https://nirvashare.com/

▲ **What Cloud Storage providers are supported by NirvaShare?**

NirvaShare supports prominent Cloud storage providers like AWS S3, Google Cloud, Azure Blob, Digital Ocean Spaces, MinIO, Backblaze B2, Oracle, Linode, Wasabi and many others.

Source: https://nirvashare.com/faqs/

4

NirvaShare With Wasabi

📅 Updated on 20 Jun 2024 · 🕐 2 Minutes to read   🖨 Print   ↩ Share   📄 PDF

How do I use NirvaShare with Wasabi?
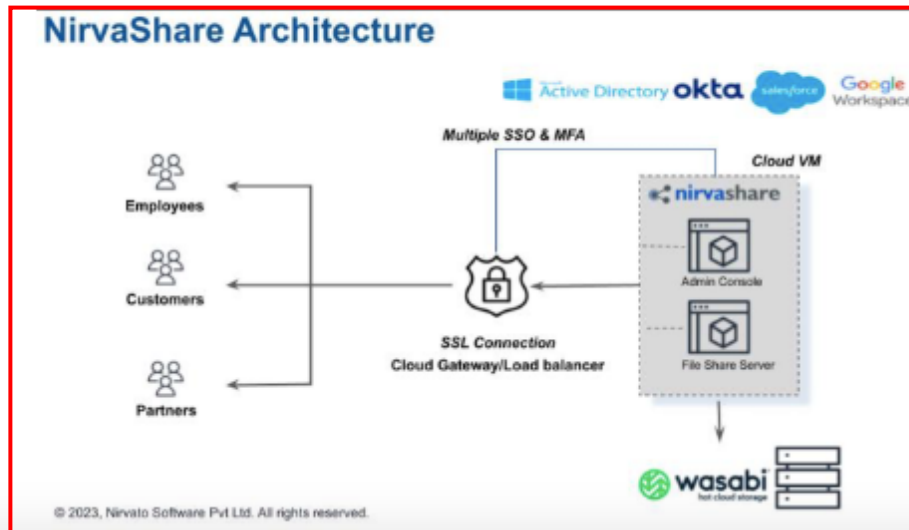
Wasabi's object storage has been validated to be used with NirvaShare.

NirvaShare is a Secure File Sharing & Access Management Solution for Wasabi's object storage. It provides an easy SSO integration with identity providers like Active Directory, Okta, etc.

1. Prerequisites

- NirvaShare version 2.4.0 and above is installed.

- An active Wasabi cloud storage account.

2. Architecture Diagram

5

Source: https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi

Storing Objects in a Bucket

media content

You can store objects in a bucket in Wasabi. An object can be any type of file—text, photo, video, etc. See Step 2 in _Getting Started: Working with a Bucket._

Source: https://docs.wasabi.com/docs/storing-objects-in-a-bucket (annotated)

About

Enterprise Secure File Sharing of Cloud Storage such as AWS S3, Azure, Wasabi, Digital Ocean Space, MinIO, and Linode is simplified now!
Securely share and collaborate any folder or file with external identities such as customers, partners, vendors, etc with security and fine access control including internal identities like employees.
Supports variety of authentication options such as Federated SSO (SAML2), Basic, Form and OTP based. Integrates with identity providers like GSuite, Active Directory, Salesforce, Okta, WordPress, and AWS SSO.

NirvaShare is an enterprise secure file sharing software featuring document copy protect, branding, digital signature, IP white listing, auditing, etc.

Source: https://www.youtube.com/channel/UCP8znBILQ0b_2ixAak_iDcw

6

Source: https://nirvashare.com/how-to-share-file-folder-and-manage-access-to-wasabi-storage/

Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: https://nirvashare.com/white-papers/

Source: https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi (annotated)

Source: https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi (annotated)

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

| [7.1] receiving a request message including media data indicating requested media content and a consumer device identifier corresponding to the consumer device; | Company performs and/or induces others to perform the step of receiving a request message including media data indicating requested media content and a consumer device identifier corresponding to the consumer device.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, Wasabi integrates NirvaShare for secure file sharing and access management from the Wasabi Cloud. NirvaShare allows file owners to share files via a URL and apply authentication measures, such as basic authentication, to control access. When a file owner shares the URL with a user, the user must authenticate using a username and password ("a consumer device identifier") upon accessing the link. Therefore, upon information and belief, when the user opens the shared URL, a request is generated containing authentication data and information about the shared file ("media data indicating requested media content"). |
|---|---|

NirvaShare With Wasabi

📅 Updated on 20 Jun 2024 · 🕐 2 Minutes to read   🖨 Print   📤 Share   📄 PDF
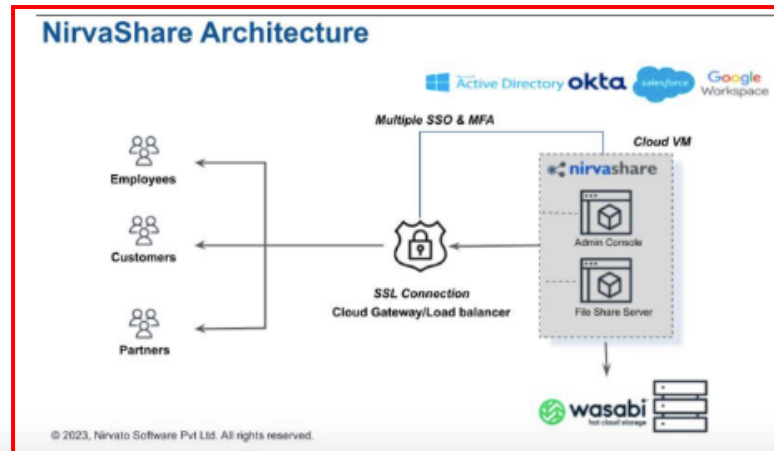
How do I use NirvaShare with Wasabi?

Wasabi's object storage has been validated to be used with NirvaShare.

NirvaShare is a Secure File Sharing & Access Management Solution for Wasabi's object storage. It provides an easy SSO integration with identity providers like Active Directory, Okta, etc.

1. Prerequisites

- NirvaShare version 2.4.0 and above is installed.

- An active Wasabi cloud storage account.

2. Architecture Diagram

Source: https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi

12

Sharing A File Or Folder

Sharing a File/Folder from object storage with users can be done by creating a Share and granting restrictive access to it. In this document, we will walk you through creating a new Share, setting access permissions, and sharing the same with users.

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

▲ **Can we share any file or folder?**

Yes, any folder or single file can be shared to users. Each share can have access rights.

Source: https://nirvashare.com/faqs/

13

New Share

From the NirvaShare Admin Console, click on the **Storage** tab from the left menu and browse through the files. Select any file or folder and right-click to get the context menu. Select **Share** to create a new share.
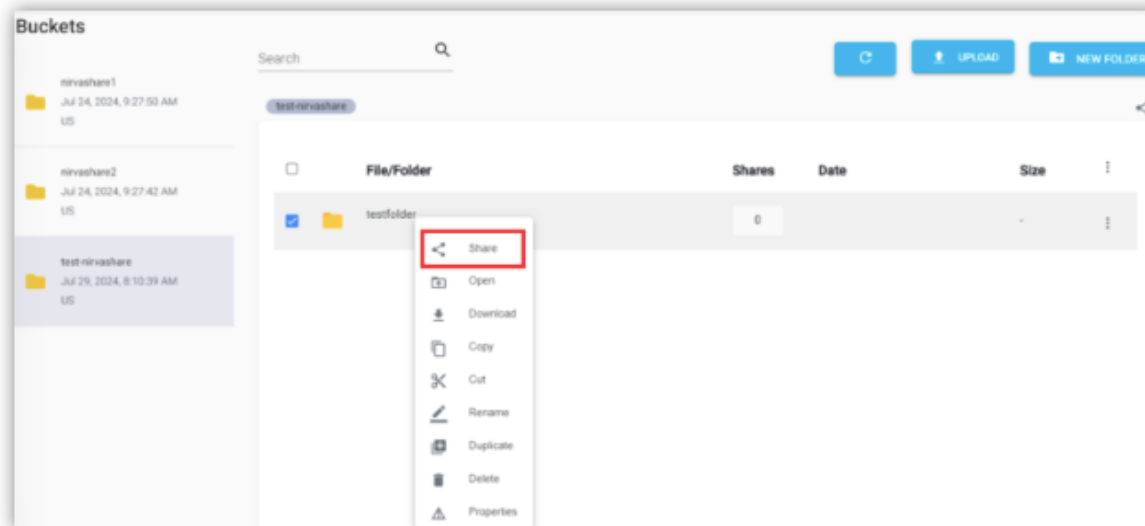
Provide a name and description for the **Share**. Before clicking on **Create Share,** move to the next tabs to set other configurations.

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

14

Authentication

Authentication can be set for the shared files. When users access this shared URL, authentication will be performed depending on the type that was set here. Supported authentication types are Basic, Form (single user), Form (multi users), OTP, FTPS and External IDP integration.

Basic Info	Permissions	Authentication	Duration

○ None (No Access)
○ Public Access
○ Basic Authentication (Single User)
○ Form Based (Single User)
○ Form Based (Multiple Access Users)
○ External Single Sign-On (SSO)
◉ One-time Password (OTP)
○ FTPS

Select Existing Login Profile *
otp ▼   New

CANCEL   CREATE SHARE

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

15

Basic Authentication – It provides old method of browser based username password way of authentication. The credentials are passed with http header after encoding.

A consumer device identifier corresponding to the consumer device

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ (annotated)

Verification

- For verifying the above procedure pertaining to file sharing, Copy the **Shareable Link** from the shares.
- Open the link in browser tab. This will redirect to Form based authentication.
- Once the authentication is effective, you should be able to access **Shares** assigned to the login profile.
- This link can be emailed or shared with your users.

Source: https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

[7.2] determining whether the consumer device identifier corresponds to a registered consumer	Company performs and/or induces others to perform the step of determining whether the consumer device identifier corresponds to a registered consumer device. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, to access the shared URL, NirvaShare requires users to authenticate according to the authentication method set by the file owner, such as basic authentication. Therefore, it would be apparent to a person having ordinary skills in the art that when the recipient of the shared files completes authentication, NirvaShare verifies the user ("determining whether the consumer device identifier corresponds to a registered consumer device") based on the provided username and password ("the consumer device identifier").

16

device; and; if it is determined that the consumer device identifier corresponds to the registered consumer device, then:	**Basic Authentication** – It provides old method of browser based username password way of authentication. The credentials are passed with http header after encoding. the consumer device identifier Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ (annotated) Verification — determining whether the consumer device identifier corresponds to a registered consumer device • For verifying the above procedure pertaining to file sharing, Copy the **Shareable Link** from the shares. • Open the link in browser tab. This will redirect to Form based authentication. • Once the authentication is effective, you should be able to access **Shares** assigned to the login profile. • This link can be emailed or shared with your users. Source: https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/ (annotated) Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.
[7.3] determining, whether the request message is one of a storage request message and	Company performs and/or induces others to perform the step of determining, whether the request message is one of a storage request message and a content request message. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, after signing in, when the user accesses the shared URL, NirvaShare displays the shared files. Additionally, NirvaShare allows the file owner to define access-level permissions, such as 'can download folder' and 'view with copy protect'. Therefore, it would be apparent to a person having ordinary skills in the art that once the files are shared with these access levels, NirvaShare provides the user with options to view or download them. If the user selects the view option ("a content request message"), NirvaShare opens and displays the file, while if the user selects the download

17

a content request message; and;	option ("a storage request message"), NirvaShare downloads the file for the user. Hence, NirvaShare performs the step of determining, whether the request message is one of a storage request message and a content request message. ## Access Levels Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks. Source: https://nirvashare.com/white-papers/

18

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

A storage request message

A content request message

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ (annotated)

19

	## Verification • For verifying the above procedure pertaining to file sharing, Copy the **Shareable Link** from the shares. • Open the link in browser tab. This will redirect to Form based authentication. • Once the authentication is effective, you should be able to access **Shares** assigned to the login profile. • This link can be emailed or shared with your users. Source: https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/ Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.
[7.4] if the request message is the storage request message, then determining whether the requested media content is available for storage; and	Company performs and/or induces others to perform the step wherein if the request message is the storage request message, then determining whether the requested media content is available for storage. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, Nirvashare enables file owners to share file through a URL with access-level permissions such as 'view with copy protect' or 'can download folder'. Therefore, upon information and belief, when the user with whom the files are shared, requests to download a file, Nirvashare verifies the associated permissions to determine whether the file can be downloaded ("determining whether the requested media content is available for storage") or if access is restricted to viewing only.

Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: https://nirvashare.com/white-papers/

<table>
<tr>
<td></td>
<td>
A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ (annotated)

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.
</td>
</tr>
<tr>
<td>[7.5] if the request message is the content request message, then</td>
<td>
Company performs and/or induces others to perform the step wherein if the request message is the content request message, then initiating delivery of the requested media content to the consumer device.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.
</td>
</tr>
</table>

initiating delivery of the requested media content to the consumer device;	For example, when the user with whom the files are shared requests to view them ("if the request message is the content request message"), the Nirvashare platform delivers the files by displaying them on the user's device ("initiating delivery of the requested media content to the consumer device"). A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma. Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ (annotated)

Storing Objects in a Bucket

media content

You can store objects in a bucket in Wasabi. An object can be any type of file—text, photo, video, etc. See Step 2 in _Getting Started: Working with a Bucket._

Source: https://docs.wasabi.com/docs/storing-objects-in-a-bucket (annotated)

Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: https://nirvashare.com/white-papers/

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

[7.6] wherein the media data includes time data that indicates a length of time to store the requested media content; and	Company performs and/or induces others to perform the step wherein the media data includes time data that indicates a length of time to store the requested media content. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, Nirvashare enables file owners to share files with a predefined expiration period ("the media data includes time data"), ensuring that the shared files remain accessible for the duration set by the file owner. Once this period expires, access to the shared files is automatically revoked, preventing further downloads or viewing. Therefore, upon information and belief, the specified time frame in which the user (with whom the files are shared) can download the file indicates a length of time to store the requested media content. Optionally, you can also set a specific duration for the share after which it becomes inactive by specifying the from and to dates in the duration tab. **CREATE NEW SHARE** Path: elasticbeanstalk-ap-south-1-100674486567/test folder/ Basic Info Permissions Authentication Duration ○ Public Access ○ Basic Authentication ◉ Form based Authentication ○ External Auth Provider ○ OTP Select a credential Form 1 New Setup Guide 4 CREATE SHARE CANCEL Source: https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi

	Duration Start and end date can be specified for the **Share** validity period, which will make **Share** to be available only for the specified duration. the media data includes time data Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/ Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.
[7.7] the first processor is further configured to determine	Company performs and induces others to perform the step wherein the first processor is configured to determine whether the requested media content exists. This element is infringed literally, or in the alternative, under the doctrine of equivalents.

26

whether the requested media content exists; and	For example, Nirvashare allows file owners to share files with a specified expiration period, ensuring that shared files and folders remain accessible for a set duration. Additionally, shared files are assigned access-level permissions such as 'view with copy protect' or 'can download folder'. Therefore, it would be apparent to the person having ordinary skills in the art that Nirvashare utilizes a processor to determine whether the requested file has 'view with copy protect' access, 'can download folder' access, or if the file's access period has expired ("the first processor is configured to determine whether the requested media content exists"). Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

27

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: https://nirvashare.com/white-papers/

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

| [7.8] if the processor determines that the requested media content exists, the processor is further configured to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to | Company performs and induces others to perform the step wherein, if the processor determines that the requested media content exists, the processor is further configured to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, Nirvashare allows file owners to apply access restrictions based on the user's IP address ("restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device"). Further, it enables the file owners to set restrictions such as to only view or both view and download the files. Therefore, it would be apparent to a person having ordinary skills in the art that Nirvashare utilizes the processor to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device. |

the consumer device.	< All Topics Main > Administrative Guide > Access Restriction with IP Address
	## Access Restriction With IP Address While sharing a file/folder with users, access can be restricted to certain white listed IP or a range of IP addresses. In this guide, we will walk you through on how to set the IP address. ## Login Profile Access Restriction can be set in the Login Profile created in NirvaShare. When a user tries to access the Shares, the login will proceed only if the user originating client IP matches the one mentioned in Access Restriction. Below are the steps to set the IP Access Restriction. - While creating or editing existing Login Profile, click on the Access tab, set the IP address in the text box of **IP Address Restriction**. - The valid format is the single IP address or can be IP range in IPv4 format. - For single IP, enter the IP address. Example *49.207.200.108* - For an IP range, enter two IP range addresses. Example *49.207.200.100 – 49.207.200.120* - For more than one IP, a range can be specified and each of them should be separated by a comma. Example *49.207.200.45, 49.105.100.12* Source: https://nirvashare.com/docs/administrative-guide/access-restriction-with-ip-address/

restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device

Source: https://nirvashare.com/docs/administrative-guide/login-profiles/login-profile-form-based-authentication/ (annotated)

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

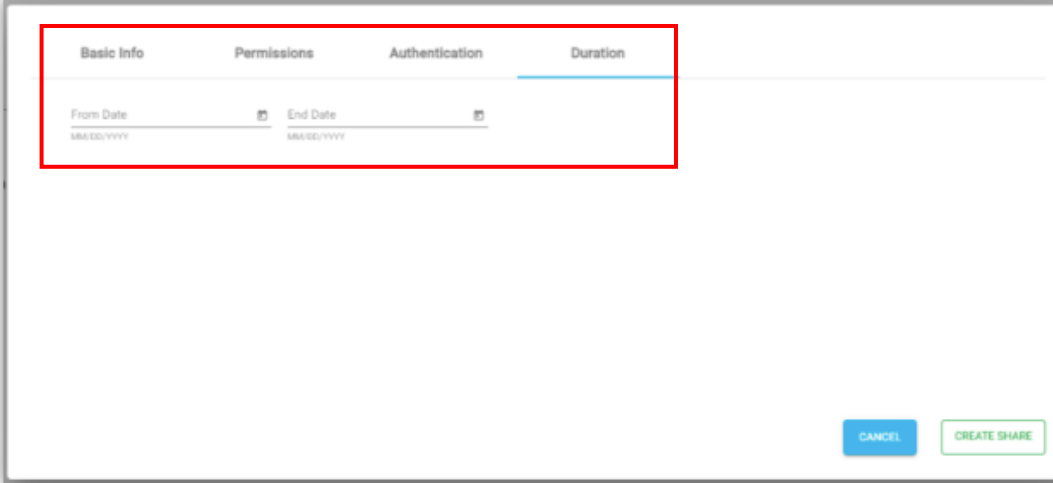Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: https://nirvashare.com/white-papers/

Source: https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

2. List of References

1. https://wasabi.com/cloud-object-storage, last accessed on 12 February 2025.
2. https://docs.wasabi.com/v1/docs/wasabi-cloud-storage-console-1, last accessed on 12 February 2025.
3. https://nirvashare.com/, last accessed on 12 February 2025.
4. https://nirvashare.com/faqs/, last accessed on 12 February 2025.
5. https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi, last accessed on 12 February 2025.
6. https://docs.wasabi.com/docs/storing-objects-in-a-bucket, last accessed on 12 February 2025.
7. https://www.youtube.com/channel/UCP8znBILQ0b_2ixAak_iDcw, last accessed on 12 February 2025.
8. https://nirvashare.com/how-to-share-file-folder-and-manage-access-to-wasabi-storage/, last accessed on 12 February 2025.
9. https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/, last accessed on 12 February 2025.
10. https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/, last accessed on 12 February 2025.
11. https://nirvashare.com/white-papers/, last accessed on 12 February 2025.
12. https://nirvashare.com/docs/administrative-guide/access-restriction-with-ip-address/, last accessed on 12 February 2025.
13. https://nirvashare.com/docs/administrative-guide/login-profiles/login-profile-form-based-authentication/, last accessed on 12 February 2025.